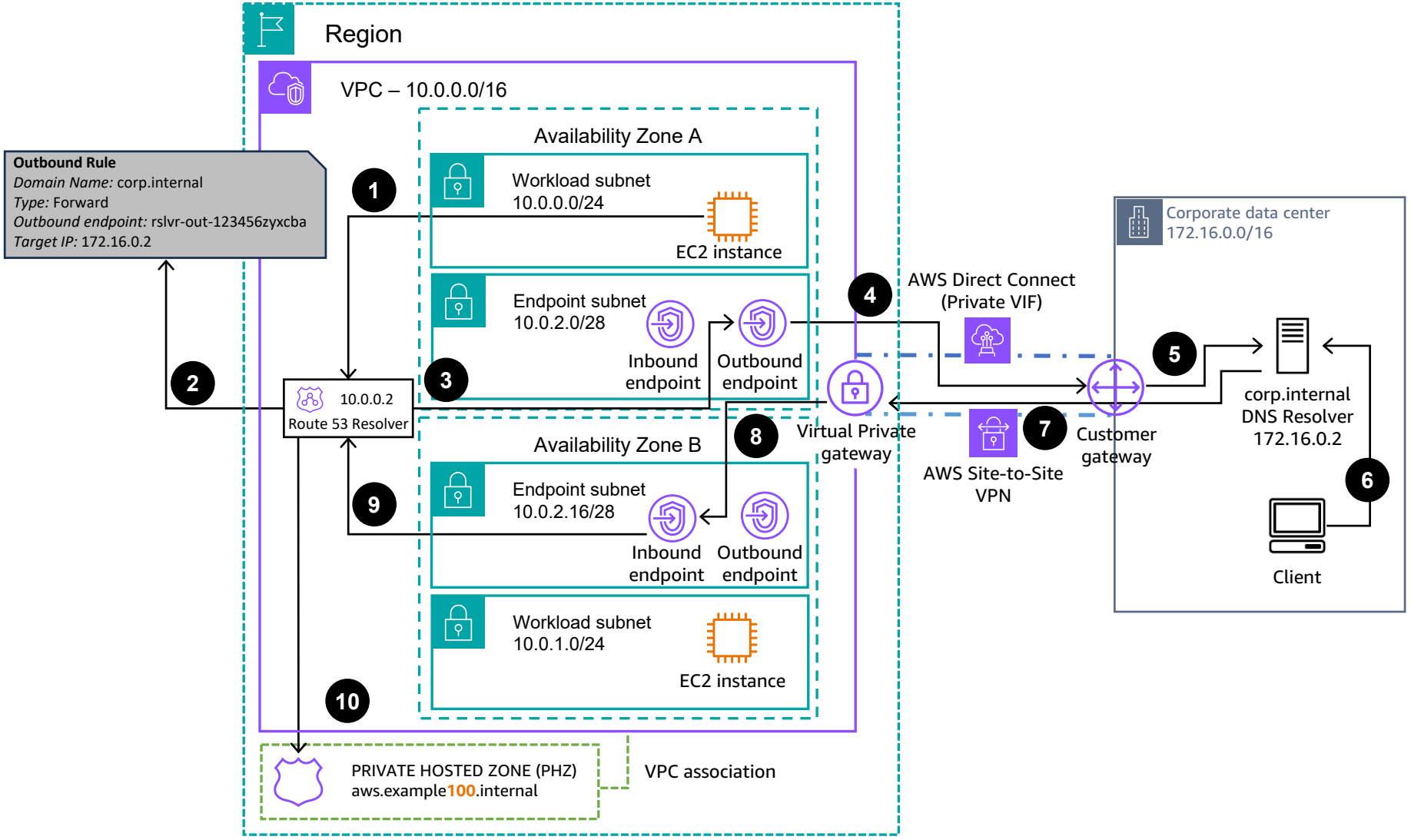
# Hybrid DNS resolution with Amazon Route 53 Resolver Endpoints (IPv4)

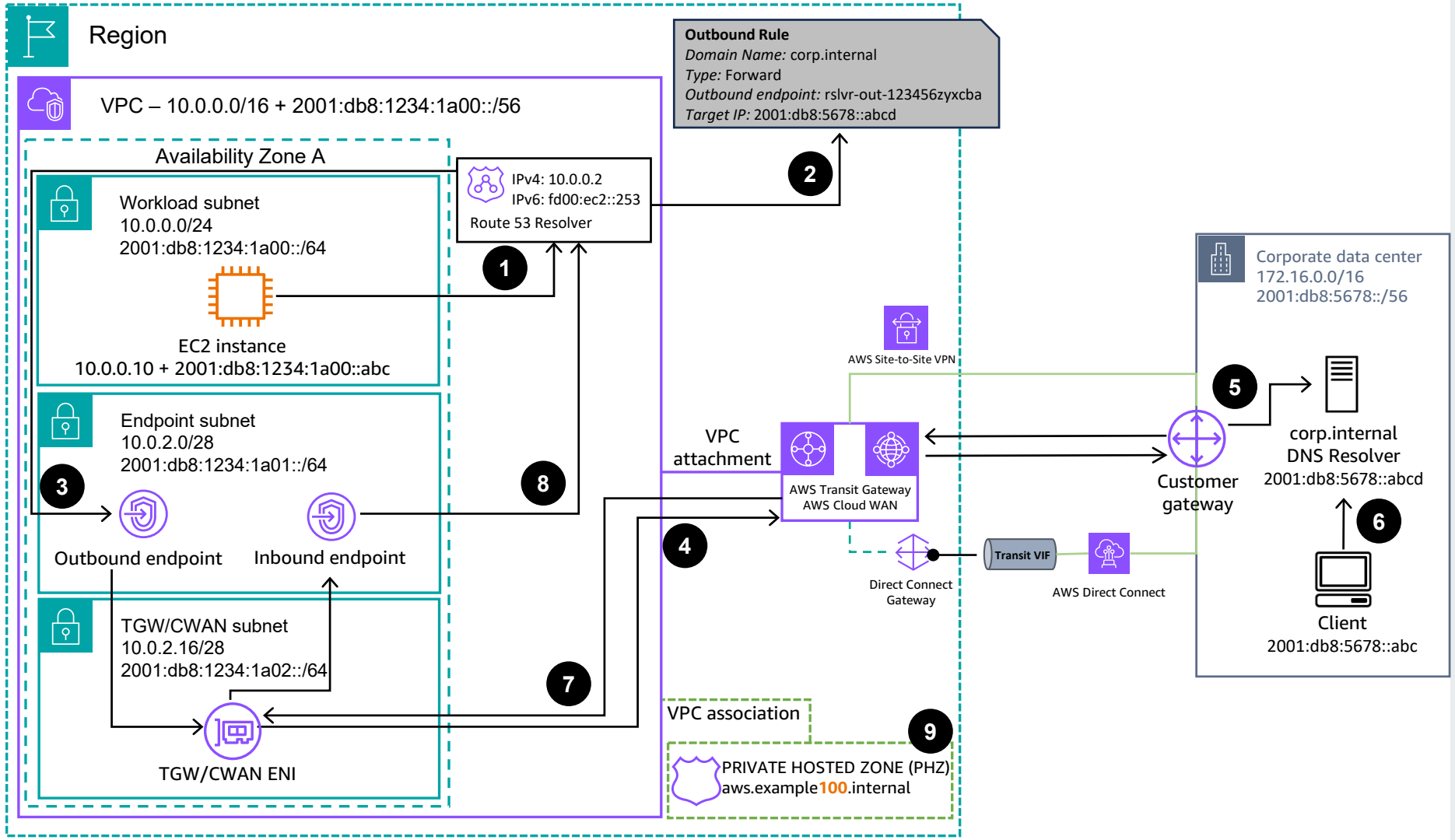



1. An **Amazon Elastic Compute Cloud (Amazon EC2)** instance needs to resolve the domain name "corp.internal". The authoritative domain name service (DNS) for this domain name is located at the corporate data center. The DNS query is sent to **Route 53 Resolver** in the VPC.
2. A Route 53 Forwarding rule is configured to forward any DNS query for "corp.internal" to the corporate data center.
3. The DNS query is sent to the **Route 53 Resolver Outbound Endpoint**.
4. The Route 53 Resolver Outbound Endpoint forwards the query to the on-premises DNS Resolver over the private connection between AWS and the corporate data center – either using AWS Direct Connect or AWS Site-to-Site VPN.
5. DNS resolution for corp.internal domain names is carried out by the DNS Resolver located in the corporate data center.
6. A client located in the corporate data center needs to resolve an "aws.example100.internal" domain name. It sends the query to its pre-configured DNS Resolver.
7. The DNS Resolver in the Corporate data center has a forwarding rule that points any DNS query for "aws.example100.internal" DNS domains to the **Route 53 Resolver Inbound Endpoint**.
8. The forwarded query arrives at the Route 53 Resolver Inbound Endpoint through either AWS Direct Connect or an AWS Site-to-Site VPN, as noted before.
9. The Route 53 Resolver Inbound Endpoint sends the query to the Route 53 Resolver within the VPC.
10. The Private Hosted Zone associated with the VPC holds the DNS records for "aws.example100.internal", so the Route 53 Resolver can resolve the query.



**AWS Reference Architecture**

# Hybrid DNS resolution with Amazon Route 53 Resolver Endpoints (dual-stack)




1. An **Amazon Elastic Compute Cloud (Amazon EC2)** instance in the dual-stack subnet makes an AAAA DNS query for *app.corp.internal* and sends it to the Route 53 Resolver in the VPC.
2. A Route 53 Forwarding rule is configured to forward any DNS query for *corp.internal* to the corporate data center. The DNS query is sent to the
3. IPv6 addresses of the **Route 53 Resolver Outbound Endpoint**.
4. The Route 53 Resolver Outbound Endpoint forwards the query to the on-premises DNS Resolver. As per the VPC routing and **AWS Transit Gateway (TGW) / AWS Cloud WAN (CWAN)** routing configuration, the query is sent to corporate data center via the hybrid connection – either using **AWS Direct Connect** or **AWS Site-to-Site VPN**.
5. DNS resolution for *corp.internal* domain names is carried out by the DNS Resolver located in the corporate data center.
6. A client located in the corporate data center makes an AAAA DNS Query for *aws.example100.internal* and sends it to its on-premises DNS resolver. The DNS resolver has a conditional forwarder and forwards all DNS queries for *example100.internal* to the IPv6 addresses of the Route 53 Resolver Inbound Endpoint.
7. The forwarded query arrives at the Route 53 Resolver Inbound Endpoint through the hybrid connection and TGW/CWAN, as noted before. The
8. Inbound Endpoint sends the query to the Route 53 Resolver within the VPC.
9. The Private Hosted Zone associated with the VPC holds the DNS records for *aws.example100.internal*, so the Route 53 Resolver can resolve the query.

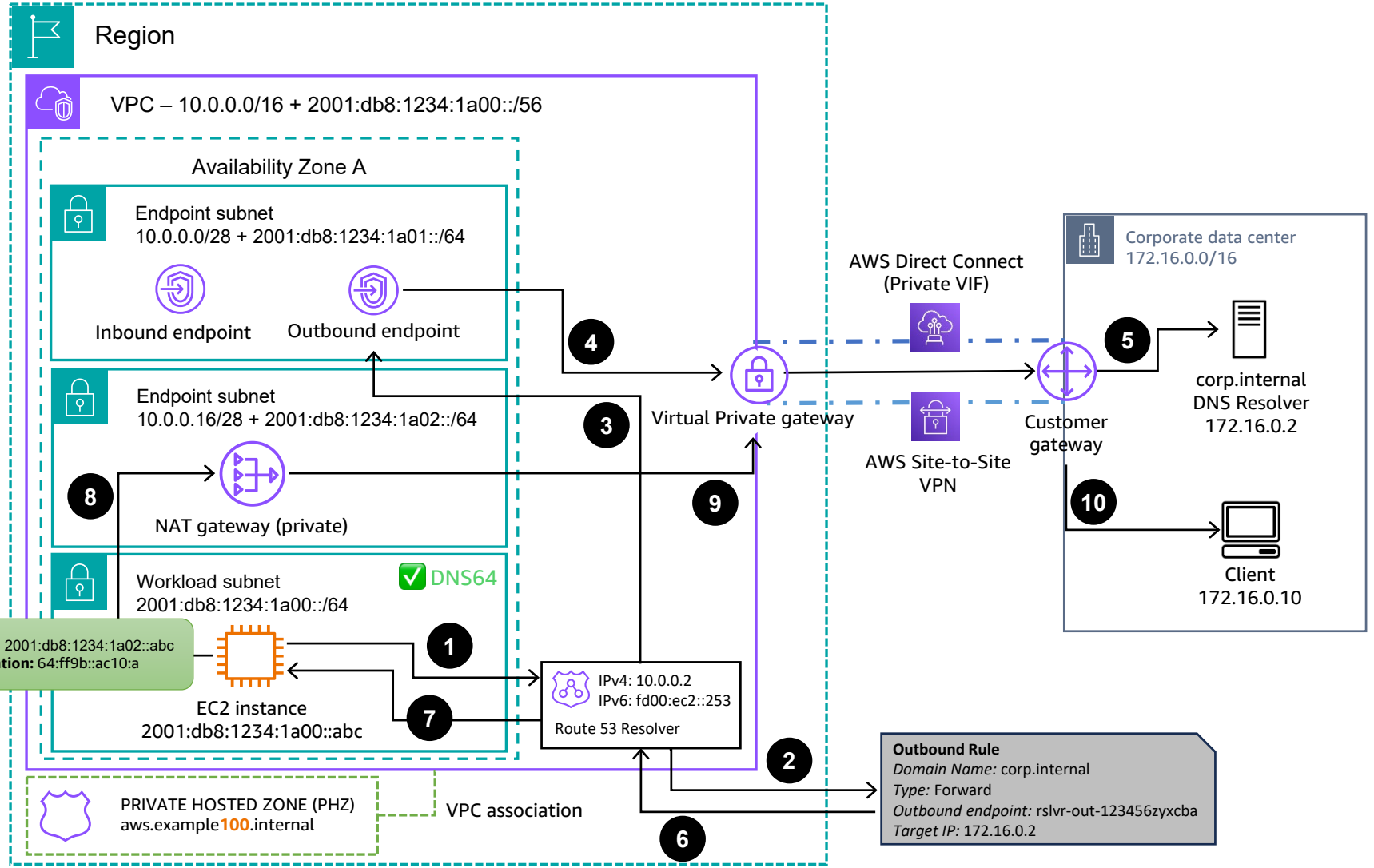
For more information about IPv6 and dual-stack architectures, check the [Dual Stack and IPv6-only Amazon VPC Reference Architectures].

For hybrid environments, check IPv6 requirements for [AWS Site-to-Site VPN] and [AWS Direct Connect].



**AWS Reference Architecture**

# Hybrid DNS resolution with Amazon Route 53 Resolver Endpoints (IPv6)

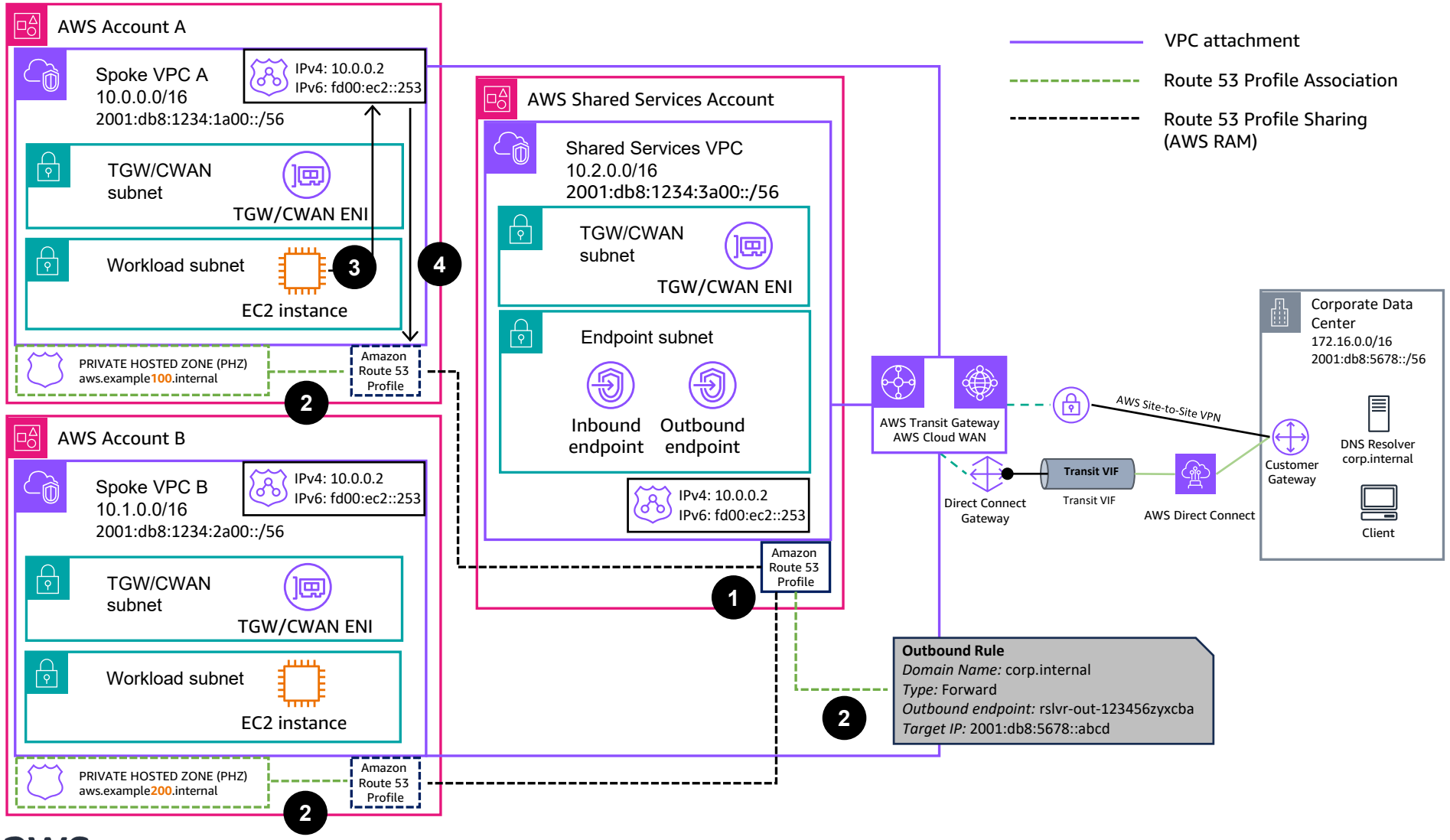



1. An **Amazon Elastic Compute Cloud (Amazon EC2)** instance in the IPv6-only subnet makes an AAAA DNS query for *app.corp.internal* and sends it to the Route 53 Resolver in the VPC.
2. A Route 53 Forwarding rule is configured to forward any DNS query for *corp.internal* to the
3. corporate data center. The DNS query is sent to the **Route 53 Resolver Outbound Endpoint**.
4. The Route 53 Resolver Outbound Endpoint forwards the query to the on-premises DNS Resolver over the private connection between AWS and the corporate data center – either using AWS Direct Connect or AWS Site-to-Site VPN.
5. DNS resolution for *corp.internal* domain names is carried out by the DNS Resolver located in the corporate data center.
6. Once the domain name has been resolved by the data center's DNS Resolver, the Route 53
7. Resolver synthesizes an IPv6 address by prepending 64:ff9b::/96 to the IPv4 address (as DNS64 is enabled)
8. As per the VPC route table, the EC2 instance sends the traffic to the private NAT gateway
9. (NAT64 enabled), and traffic gets routed to the data center's client – either using AWS
10. Direct Connect or AWS Site-to-Site VPN.



**AWS Reference Architecture**

# Multi-Account and multi-VPC Hybrid DNS resolution using Amazon Route 53 Profiles




1. An Amazon Route 53 Profile is created in the Shared Services account, and shared via AWS Resource Access Manager (RAM) to Accounts A and B. When sharing a Route 53 Profile, it can be done with read-only or admin permissions. In this case, it was done with admin permissions, so Accounts A and B can also associate resources.

2. The Route 53 profile is associated with VPCs A, B and Shared Services, so these VPCs can consume the DNS resolution configured. In addition, Accounts A and B associate a Private Hosted Zone (PHZ), and the Shared Services Account shares a Forwarding Rule.

3. An **Amazon Elastic Compute Cloud (Amazon EC2)** instance query the Route 53 Resolver in the VPC for domain name resolution.

4. As the Route 53 Profile is associated to the VPC, any domain name within the *aws.example100.internal* and *aws.example200.internal* domain names will be resolved by the Route 53 Resolver. DNS queries within the *corp.internal* domain name will be forwarded via the Route 53 Resolver Outbound Endpoint.

For more information about IPv6 and dual-stack architectures, check the Dual Stack and IPv6-only Amazon VPC Reference Architectures.

For hybrid environments, check IPv6 requirements for AWS Site-to-Site VPN and AWS Direct Connect.

Note that you can also share Private Hosted Zones and Resolver Rules without the use of Route 53 Profiles.



**AWS Reference Architecture**